



September 2026

INTERNET OF THINGS

OMB Action Needed to Ensure Agencies Secure Their Networked Devices



OMB Action Needed to Ensure Agencies Secure Their Networked Devices

GAO-26-108937

September 2026

A report to congressional committees

Contact: David B. Hinchman at hinchmand@gao.gov

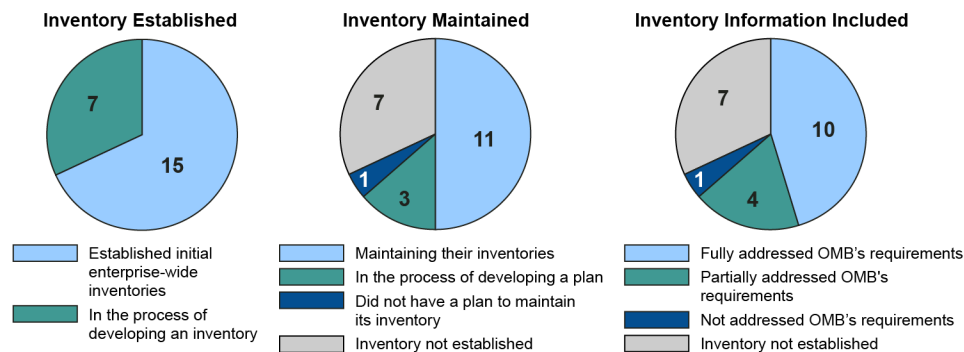
What GAO Found

The nation's infrastructure relies on information systems to support its varied functions. This includes the networked Internet of Things (IoT) and operational technology (OT) devices that interact with the physical world, including in building maintenance systems and specialized equipment in hospitals and laboratories.

Responsible federal agencies have issued guidance, best practices, and requirements to help agencies securely procure such devices. For example, the Office of Management and Budget (OMB) has issued requirements to ensure that agencies establish and maintain inventories of their networked devices and process IoT cybersecurity waivers.

However, most agencies have not fully addressed OMB's networked device requirements, which were established in December 2023 and updated in January 2025. Specifically, agencies' initial inventories were required to be completed by September 2024. However, as of September 2026, of the 22 civilian Chief Financial Officer (CFO) Act agencies in GAO's review, 15 had established an inventory, 11 were maintaining their inventories, and 10 had included all required information (such as asset description and software version) for each device. Overall, only seven agencies had fully addressed all three of OMB's requirements. Further, no agencies had reported an IoT cybersecurity waiver.

Status of 22 Agency Networked Device Inventories, as of September 2026



Source: GAO analysis of Chief Financial Officer (CFO) Act agency documentation. | GAO-26-108937

Agencies cited a variety of reasons for not having completed or maintained inventories with required information, including technical and resource constraints and competing priorities. However, OMB has yet to issue updated guidance to agencies that covers fiscal year 2026, leaving agencies without a clear imperative to prioritize implementation of the requirements and a timeline for doing so. Until OMB issues this guidance, agencies will lack appropriate direction on how and when to complete their device inventories. In the absence of inventories, agencies may lack awareness of the number and type of connected devices in their systems and be at risk of not protecting those systems from cyberattacks. Further, without updated guidance and oversight of agencies' implementation of inventory requirements, agencies may continue to struggle to apply appropriate security controls to vulnerable systems—potentially compromising highly sensitive data and systems.

Why GAO Did This Study

Networked technologies and devices are facing increasing cyber threats from around the globe. For example, in July 2026, cyber threat actors disrupted operations in the water sector by modifying passwords to disconnect networked programmable logic controllers, which are a type of OT. Moreover, emerging technologies such as artificial intelligence can compound risks faced by these technologies and devices. The IoT Cybersecurity Improvement Act of 2020 includes provisions for OMB and civilian CFO Act agencies to identify and protect networked devices.

The act also includes provisions for GAO to report every 2 years on IoT guidance and the waiver process through 2026. This final report in a series of three (1) describes guidance and best practices for procuring secure networked devices; and (2) evaluates agencies' progress in addressing networked device cybersecurity.

GAO identified federal agencies with cybersecurity or acquisition responsibilities and described guidance and best practices developed by those agencies for procuring secure networked devices. GAO compared 22 civilian CFO Act agencies' inventory implementation efforts to OMB's requirements. GAO also interviewed relevant agency officials to obtain their views and verify the information provided.

What GAO Recommends

GAO recommends that OMB issue updated cybersecurity guidance for networked IoT and OT devices and oversee agencies' implementation of the requirements. OMB did not provide comments on this report.

Contents

Letter		1
	Background	5
	Guidance and Best Practices Can Assist Agencies in Securely Procuring Networked Devices	15
	Most Agencies Have Not Fully Addressed OMB's Networked Device Cybersecurity Requirements	19
	Conclusions	28
	Recommendation for Executive Action	29
	Agency Comments	29
Appendix I	Prior GAO Recommendations Related to the Internet of Things Cybersecurity Improvement Act of 2020	32
Appendix II	Key National Institute of Standards and Technology Publications	36
Appendix III	Extent to Which Agencies Have Implemented Networked Device Inventory Information Requirements	38
Appendix IV	GAO Contact and Staff Acknowledgments	40
Tables		
	Table 1: Status of Agencies' Efforts to Develop and Maintain Inventories of Networked Internet of Things (IoT) and Operational Technology (OT) Devices, as of September 2026	24
	Table 2: Open Recommendations on Addressing Internet of Things (IoT) Legislative Requirements from GAO-25-107179, as of August 2026	33
	Table 3: Open Recommendations on Addressing Internet of Things (IoT) Legislative Requirements from GAO-23-105327, as of August 2026	34

Table 4: Key National Institute of Standards and Technology (NIST) Publications Providing Guidelines for the Secure Procurement of Internet of Things (IoT) and Related Devices, as of July 2026	36
Table 5: Extent to Which Chief Financial Officers (CFO) Act Agencies Included Eight Categories of Information Required by OMB in Their Networked Device Inventories, as of September 2026	38

Figures

Figure 1: Information Technology (IT), Internet of Things (IoT), and Operational Technology (OT)	7
Figure 2: Office of Management and Budget's (OMB) Information Requirements for Agency Inventories of Networked Devices	20
Figure 3: Chief Financial Officer (CFO) Act Agency Progress in Establishing Initial Inventories of Networked Internet of Things (IoT) and Operational Technology Devices from December 2024 Through September 2026	21
Figure 4: Agency Efforts to Develop and Maintain Inventories of Networked Internet of Things (IoT) and Operational Technology (OT) Devices and Include All Required Information, as of September 2026	22

Abbreviations

CFO Act	Chief Financial Officers Act
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FAR Council	Federal Acquisition Regulatory Council
FISMA	Federal Information Security Modernization Act
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IoT	Internet of Things
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OT	operational technology
SBA	Small Business Administration
SRMA	sector risk management agency
SSA	Social Security Administration
USAID	United States Agency for International Development
USDA	U.S. Department of Agriculture

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 30, 2026

Congressional Committees

The critical infrastructure of the nation, including electricity, health care, and transportation, underpins American society.¹ This infrastructure relies on networked Internet of Things (IoT) and operational technology (OT) devices to support its varied functions. IoT generally refers to the technology and devices that allow for the connection and interaction of “things” throughout such places as buildings and vehicles. OT devices interact with the physical world, including in building maintenance systems, environmental sensors, and specialized equipment in hospitals and laboratories.

The risks facing technologies such as IoT and OT include escalating threats from around the globe, the emergence of new and more destructive attacks, and insider threats from witting or unwitting employees. Recent incidents—such as a cyberattack on Poland’s energy sector in which a cyber threat actor gained access to internet-connected devices, damaged remote units, disrupted control between facilities and distribution system operators, destroyed data, and corrupted firmware on connected devices—highlight the risks posed by these systems.² Moreover, emerging technologies such as artificial intelligence can compound risks faced by these technologies and devices. We have previously reported that threat actors have increasingly used artificial intelligence to accelerate attacks against critical infrastructure systems.³ The prevalence and wide range of IoT and related devices used by

¹The term “critical infrastructure” refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government services and facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

²For further details, see Cybersecurity and Infrastructure Security Agency, *Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps* (Feb. 10, 2026), accessed February 10, 2026, [Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps | CISA](#).

³GAO, *Artificial Intelligence: DHS Needs to Improve Risk Assessment Guidance for Critical Infrastructure Sectors*, [GAO-25-107435](#) (Washington, D.C.: Dec. 18, 2024).

federal agencies also provides new and more complex vectors for cyber incidents. Agencies must be aware of the devices connected to their systems to understand and respond to their potential cybersecurity risks.

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we first designated federal information security as a government-wide High Risk area in our biennial report to Congress in 1997.⁴ In 2003, we expanded this High Risk area to include the protection of critical cyber infrastructure.⁵ We continue to identify the protection of critical cyber infrastructure as a High Risk area, as shown in our February 2025 High Risk update on major cybersecurity challenges.⁶

The IoT Cybersecurity Improvement Act of 2020⁷ includes requirements for the National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and federal agencies.⁸ Additionally, the act establishes specific provisions for Chief Financial Officers (CFO) Act

⁴GAO, *High-Risk Series: An Overview*, [HR-97-1](#) (Washington, D.C.: Feb. 1, 1997).

⁵GAO, *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: Jan. 1, 2003).

⁶GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, [GAO-25-107743](#) (Washington, D.C.: Feb. 25, 2025).

⁷Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 134 Stat. 1001 (Dec. 4, 2020), codified at 15 U.S.C. §§ 278g-3a – 3e. The statute is also named the IoT Cybersecurity Improvement Act of 2020.

⁸The IoT Cybersecurity Improvement Act of 2020 defines “agency” broadly (Pub. L. No. 116-207, § 3(1) (15 U.S.C. § 278g-3a), using the definition of “agency” at 44 U.S.C. § 3502).

agencies other than the Department of Defense.⁹ It also includes provisions for GAO to report biennially for the six years following the law's enactment on efforts to enhance the cybersecurity of IoT, including IoT procurement guidance and the effectiveness of OMB's process for waiving selected IoT cybersecurity requirements.¹⁰ We previously issued our first two reports required under the act in December 2022 and December 2024.¹¹ This third and final report in the series (1) describes guidance and best practices for procuring secure networked devices; and (2) evaluates agencies' progress in addressing networked device cybersecurity and IoT waiver requirements.

To address our first objective, we used our most recent report under the act as a baseline¹² and described guidance and best practices—including any updates since our last report—for procuring secure networked devices as identified by federal agencies with government-wide cybersecurity acquisition or oversight responsibilities. These agencies include OMB, NIST, the Department of Homeland Security (DHS), and the Federal Acquisition Regulatory Council (FAR Council). As in our past work, we then identified and described guidance, recommended best

⁹Certain key provisions of the IoT Cybersecurity Improvement Act of 2020 are linked to the Chief Information Officer (CIO) reviews required by the Federal Information Technology Acquisition Reform Act (FITARA) of the 23 civilian agencies covered by the Chief Financial Officers Act of 1990. See Pub. L. No. 106-207, § 7 (15 U.S.C. § 278g-3e), referencing the review required by 40 U.S.C. § 11319(b)(1)(C) of these agencies (40 U.S.C. sec. 11319(a)(1), as added by Pub. L. No. 113-291, § 831(a)). For this reason, the scope of our review includes these 23 agencies, which are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. 31 U.S.C. sec. 901(b). We did not include the Department of Defense in our review because it is not covered by the relevant FITARA review provisions (40 U.S.C. § 11319(b)(1)(C), “[a] covered agency other than the Department of Defense”) and is thus not included in the procurement and use prohibition and waiver provisions of the IoT Cybersecurity Improvement Act of 2020 linked to the FITARA review provisions (see 15 U.S.C. § 278g-3e(a)(1), (b)).

¹⁰Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, § 7(c), 134 Stat. 1001, 1006 (Dec. 4, 2020).

¹¹See the initial report at GAO, *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, [GAO-23-105327](#) (Washington, D.C.: Dec. 1, 2022) and the second report at GAO, *Internet of Things: Federal Actions Needed to Address Legislative Requirements*, [GAO-25-107179](#) (Washington, D.C.: Dec. 4, 2024).

¹²[GAO-25-107179](#).

practices, directives, and regulations for the acquisition of technologies, including IoT, issued by these agencies. We validated them with the agencies and made changes as appropriate.

To address our second objective, we compared the 22 civilian CFO Act agencies' efforts to implement networked device cybersecurity and IoT waiver requirements to OMB's requirements related to the act.¹³ To identify OMB's requirements for IoT cybersecurity related to the act, we evaluated OMB's memoranda in fiscal years 2023, 2024, and 2025 implementing the Federal Information Security Modernization Act (FISMA) and the IoT Cybersecurity Improvement Act of 2020.¹⁴ These requirements included developing and maintaining inventories of networked IoT and OT devices and granting waivers for IoT devices that do not comply with NIST standards.¹⁵

We then evaluated documentation from the 22 civilian CFO Act agencies, such as agencies' plans for inventories of networked devices, and

¹³We did not include the U.S. Agency for International Development (USAID) in our analysis because the agency could not provide information in a timely manner for our review due to a substantial reduction in personnel. As a result, our analysis included 22 of the 23 civilian CFO Act agencies.

¹⁴Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, M-23-03 (Washington, D.C.: Dec. 2, 2022), subsequently replaced by M-24-04 on December 4, 2023. Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, M-24-04 (Washington, D.C.: Dec. 4, 2023). M-24-04 was subsequently replaced by M-25-04 on January 15, 2025. Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, M-25-04 (Washington, D.C.: Jan. 15, 2025). As of July 2026, OMB has not issued guidance for fiscal year 2026.

¹⁵OMB's December 2023 memorandum introduced the concept of "covered IoT," an administrative definition of IoT that includes some technologies that are traditionally called OT. OMB's definition of covered IoT included both IoT devices and some OT devices embedded with programmable controllers, integrated circuits, sensors, and other technologies for the purpose of collecting and exchanging data with other devices or systems over a network. OMB also noted that such devices also facilitate enhanced connectivity, automation, and data-driven insights across devices and systems. OMB noted that this was due to the identification of the convergence between IoT and OT as a potential cybersecurity risk. In January 2025, OMB dropped the use of the phrase "covered IoT" and directed agencies to inventory both networked IoT and OT devices that interact with the physical world.

agencies' FISMA quarterly reports from fiscal year 2025,¹⁶ to determine whether the agencies had implemented the requirements in the act and OMB's memoranda to develop the inventories. To determine whether agencies were maintaining the inventories, we evaluated agency plans and procedures for maintaining the inventories. For each agency, we assessed the implementation of the requirements as follows:

- **Fully Addressed:** the agency provided evidence that showed it had fully addressed the requirements.
- **Partially Addressed:** the agency provided evidence that showed it had addressed part of the requirements.
- **Not Addressed:** the agency did not provide evidence that it had addressed any part of the requirements.

Additionally, we analyzed information on the waivers the 22 civilian CFO Act agencies we reviewed reported granting under the act and under OMB's guidance. For both objectives, we met with relevant agency officials to obtain their views and verify the information provided.

We conducted this performance audit from February 2026 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Information technology (IT) and networked IoT and OT devices can work together in systems and can assist federal agencies in conducting their missions. IT includes technologies used in data processing, networking, sharing, and disposing of data, such as computers. IoT devices are connected to networks and interact with the physical world, and these devices can function on their own, in addition to when they are acting as a

¹⁶OMB did not require agencies to submit FISMA reports for the first two quarters of fiscal year 2026.

component of another system.¹⁷ For example, IoT could include smart building management devices, such as motion-activated security cameras. In addition, NIST defines OT as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).¹⁸ OT systems and devices detect or cause a direct change through the monitoring or control of other devices, processes, and events. They include controllers, sensors, and actuators, and include examples such as supervisory control and data acquisition systems, distributed control systems (like those used to automate industrial equipment), and building automation systems.

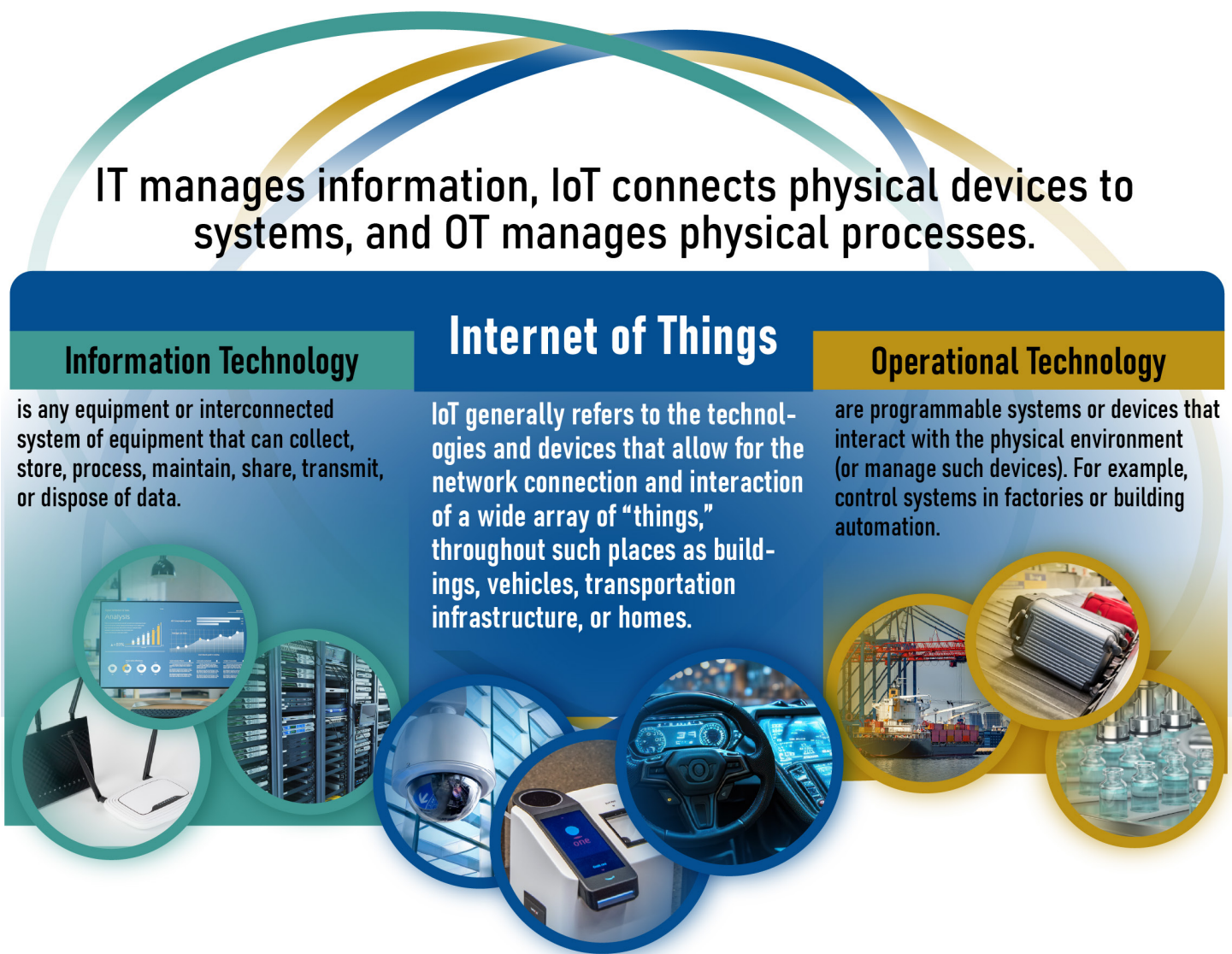
Many IoT devices incorporate technological advances like cloud computing, mobile computing, embedded systems, big data, and low-price hardware. IoT devices can provide computing functionality, data storage, and network connectivity for equipment that previously lacked them. This has enabled new efficiencies and technological capabilities for equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the abilities to analyze data about the physical world and use the results to better inform decision-making, alter the physical environment, and anticipate future events. Federal agencies use a wide variety of IoT technologies, ranging from specialized connected equipment in hospital settings to smart building management or smart road technologies. Federal agencies can also use a variety of OT, which may include industrial control systems, building automation systems, transportation systems, physical access control systems,

¹⁷The Internet of Things Cybersecurity Improvement Act of 2020 incorporates a 2020 NIST definition of IoT. It defines IoT devices as devices that “(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional IT devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.” Sensors sense the environment, while actuators are devices for moving or controlling a mechanism or system; an actuator is the mechanism by which a control system acts on its environment.

¹⁸More fully, NIST notes that OT encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. See National Institute of Standards and Technology, *Guide to Operational Technology Security, NIST Special Publication 800-82 Revision 3* (Gaithersburg, MD: September 2023).

physical environment monitoring systems, and physical environment measurement systems. See figure 1 for an overview of IT, IoT, and OT.

Figure 1: Information Technology (IT), Internet of Things (IoT), and Operational Technology (OT)



Sources: GAO analysis of government and industry information; patrikslezak/stock.adobe.com (wifi); Gorodenkoff/stock.adobe.com (computer); shock/stock.adobe.com (servers); alice_photo/stock.adobe.com (camera); Rocky Grimes/stock.adobe.com (palm reader); sirinakboakaew/stock.adobe.com (car); Александр Беспальный/stock.adobe.com (ships); Voy_ager/stock.adobe.com (baggage); wacomka/stock.adobe.com (medical). | GAO-26-108937

Cyber Threats to Networked Devices

Networked devices such as IoT and OT and the corresponding systems that support federal agencies and our nation's critical infrastructures are increasingly at risk. They are highly complex, technologically diverse, and often geographically dispersed. In addition, they are often interconnected with other internal and external systems and networks, including the internet. This complexity increases the difficulty of identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the federal government's systems and networks.

These technologies are subject to serious cyber threats that can have adverse impacts on organizational operations and assets, individuals, critical infrastructure, and the nation. As cyber threats grow increasingly sophisticated, including with the emergence of quantum computing and artificial intelligence, the need to manage and bolster the cybersecurity of networked products and services is also magnified. These cyber threats can include purposeful attacks, environmental disruptions, and machine errors, and may result in harm to the national and economic security interests of the United States. For example, a major threat is the use of botnets, which are networks of internet-connected devices infected with bot malware and remotely controlled by attackers.¹⁹ Another significant threat is a denial-of-service attack—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.²⁰ Systems may also face attacks where attackers intercept communications to steal and manipulate data or face exploits that target vulnerabilities that are not yet known to the general public.

Recent events highlight significant cyber threats to networked devices:

- In July 2026, DHS's Cybersecurity and Infrastructure Security Agency (CISA) reported that cyber threat actors targeted internet-exposed assets in the Water and Wastewater Systems sector by modifying passwords to lock out operators and disconnecting assets from its networks. These assets include network-connected programmable logic controllers, a type of OT. These instances resulted in operational impacts to water systems, including boil water notices, and forced the operators to revert to manual operations. The threat actors have

¹⁹Also known as malicious code and malicious software, malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

²⁰A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.

targeted water entities of all sizes.²¹ This follows a December 2024 joint alert from CISA and the Environmental Protection Agency, which reported that pro-Russian hackers manipulated internet-exposed devices in the Water and Wastewater Systems sector, causing water pumps and blower equipment to exceed their normal operating parameters. The hackers altered settings, turned off alarm mechanisms, and changed administrative passwords to lock out the water utility operators. These instances resulted in operational impacts to water systems and forced victims to revert to manual operations.²²

- In April 2026, CISA issued an advisory from the United Kingdom's Cyber League, the National Cyber Security Centre of the United Kingdom, and international partners.²³ It reported that a People's Republic of China state-sponsored cyber group had compromised IT and IoT networks to create botnets of routers and IoT devices, primarily with devices that were vulnerable because they were out of date and no longer receiving updates or security patches by their manufacturers. Based on past alerts, including in February 2024, these botnets have been used to target critical infrastructure sectors including the Communications, Energy, Transportation Systems, and Water and Wastewater Systems sectors. Specifically, CISA and its partner agencies noted that the threat actors appeared to be pre-positioning themselves on IT networks to enable them to move to network-connected OT assets to disrupt functions of critical infrastructure in the future.²⁴

²¹Cybersecurity and Infrastructure Security Agency, "CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs," (Jul. 30, 2026), accessed July 31, 2026, [CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs](#).

²²Environmental Protection Agency and Cybersecurity and Infrastructure Security Agency, "Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems," (Dec. 13, 2024), accessed May 14, 2026, [Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems](#).

²³National Cyber Security Centre (NCSC-UK) and international partners, including the Cybersecurity and Infrastructure Security Agency, "Defending Against China-nexus Covert Networks of Compromised Devices," accessed June 9, 2026, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a>.

²⁴Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," (Feb. 7, 2024), accessed June 4, 2026, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

IoT Cybersecurity Improvement Act of 2020

The IoT Cybersecurity Improvement Act of 2020 includes provisions for the protection of IoT owned or controlled by federal agencies²⁵ and requires NIST to develop and publish standards and guidelines for the federal government on agencies' use and management of IoT devices. In addition, the act requires OMB to review agency policies pertaining to IoT devices owned or controlled by agencies for consistency with NIST standards and guidelines. At the act's direction, OMB is then to issue policies and guidance, as necessary, to ensure agency policies are consistent with the NIST guidelines concerning IoT. OMB is also to oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including IoT devices).

Further, OMB is to establish a standardized process for agency Chief Information Officers (CIO) to use for obtaining waivers to the IoT cybersecurity requirements outlined below. Generally, before any civilian CFO Act agencies may enter or renew a contract for IT or IT services, the agency CIO must review and approve the contract, as required by law. Under the act, if during that review for a system including IoT, the CIO determines that using the device would prevent the agency from complying with NIST IoT standards and guidelines, the agency is prohibited from using the device. The agency would also be prohibited from procuring or obtaining the device or renewing a contract to procure or obtain the device.

This prohibition may be waived by the head of the agency, but only if the agency CIO first determines that at least one of the following conditions is met:

1. The waiver is necessary in the interest of national security.
2. Procuring, obtaining, or using the IoT device is necessary for research purposes.
3. The device is secured using alternative and effective methods appropriate to its function.

²⁵Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 134 Stat. 1001 (Dec. 4, 2020) codified at 15 U.S.C. §§ 278g-3a – 3e. The statute is also named the IoT Cybersecurity Improvement Act of 2020.

Federal Roles and Responsibilities for Procuring Secure IoT

Several entities within the federal government have responsibilities for helping to oversee and guide the procurement of secure IoT technologies.

OMB. The agency's responsibilities include oversight of the management of federal agencies' technologies.²⁶ According to OMB, its role and the role of the Office of the Federal CIO within OMB, are to enable agencies to adopt IT technology, including IoT and OT, in a manner that is consistent with the President's budget and that enhances the agencies' missions.²⁷ In addition, OMB includes the Office of Federal Procurement Policy. The office plays a central role in shaping the policies and practices federal agencies use to acquire the goods and services they need to carry out their responsibilities, which include IoT and OT.

DHS. The agency oversees technology-specific issues in support of the 2013 National Infrastructure Protection Plan (the National Plan), among many other responsibilities.²⁸ In this role, DHS coordinates with other federal agencies, works with private sector entities that support critical infrastructure, and contributes to the development of guidance related to security considerations when acquiring IoT devices. In addition, FISMA authorized DHS to issue binding operational directives to federal agencies, consistent with OMB's policies and guidance.²⁹ These directives require agencies to safeguard federal information and information systems, including IoT and OT devices, from a known or reasonably suspected information security threat, vulnerability, or risk.

²⁶40 U.S.C. § 11302-03 (Clinger-Cohen Act); see also 44 U.S.C. § 3504 (Paperwork Reduction Act); 44 U.S.C. § 3602 (E-Government Act); 44 U.S.C. § 3553 (Federal Information Security Modernization Act of 2014, which largely superseded the Federal Information Security Management Act of 2002).

²⁷The Federal Chief Information Officer is the Administrator of the OMB Office of Electronic Government and Information Technology, which was created by the E-Government Act of 2002. Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

²⁸Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: Dec. 2013). The plan outlines how government and private sector participants in the critical infrastructure community can work together to manage risks and achieve security and resilience outcomes for their information systems. To achieve this end, critical infrastructure partners must collectively identify national priorities, articulate clear goals, mitigate risk, measure progress, and adapt based on feedback and the changing environment.

²⁹Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3076 (Dec. 18, 2014), codified at 44 U.S.C. § 3553(b)(2).

CISA. Established within DHS by the Cybersecurity and Infrastructure Security Agency Act of 2018, CISA's responsibilities include developing and implementing information sharing programs.³⁰ Through these programs, CISA develops partnerships and shares substantive information with the private sector and state, local, tribal, and territorial governments, including information on IoT and OT threats. In addition to information sharing initiatives, CISA is also responsible for developing resources to help spread awareness about cyber threats, protective measures, and response tactics.

NIST. The agency conducts research and develops standards, guidelines, and tools for public and non-public organizations. NIST also develops security standards and guidelines for non-national security federal agency systems, which can be mandatory for federal agencies. NIST has issued multiple publications and engaged in projects to help manage the security of IoT and OT, including Special Publication (SP) 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. This guidance is intended to help federal agencies securely incorporate IoT devices into existing information systems as system elements.³¹ NIST has also published OT-specific guidance such as SP 800-82, Revision 3, *Guide to Operational Technology (OT) Security*, which is intended to help agencies apply NIST's risk management framework cybersecurity controls to OT.³²

Federal Acquisition Regulatory Council. The Federal Acquisition Regulation (FAR) is the primary regulation used by all federal executive agencies to acquire supplies and services with appropriated funds. The FAR Council, which consists of the Secretary of Defense and the Administrators of the Office of Federal Procurement Policy in OMB, the National Aeronautics and Space Administration (NASA), and the General Services Administration (GSA), assists in the direction and coordination of

³⁰The Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169 (Nov. 16, 2018), adding sec. 2202 to the Homeland Security Act of 2002, codified at 6 U.S.C. § 652.

³¹National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication (SP) 800-213 (Gaithersburg, MD: Nov. 2021). NIST issued an initial public draft of SP 800-213 revision 1 in June 2026. It focuses on IoT products, rather than specifically on devices.

³²National Institute of Standards and Technology, Special Publication (SP) 800-82 Revision 3.

government-wide procurement policy and regulatory activities. The council is responsible for maintaining the FAR and managing, coordinating, and controlling changes in the FAR. Revisions to the FAR, as discussed later in this report, are being considered based on recent NIST guidance on IoT cybersecurity, among other things.

Federal Acquisition Security Council. The Federal Acquisition Security Council was established by the Federal Acquisition Supply Chain Security Act of 2018.³³ The council is a cross-agency council responsible for providing guidance to executive agencies to reduce their information and communications technology supply chain risks, including for networked devices and systems.³⁴ The council can also recommend removal orders on specific technologies, including networked technologies, that may pose supply chain risks.³⁵

Prior GAO Reports on the Status of IoT and Cybersecurity Risks

As previously mentioned, the IoT Cybersecurity Improvement Act of 2020 includes provisions for GAO to report biennially for the six years following the law's enactment on efforts to enhance the cybersecurity of IoT, including IoT procurement guidance and the effectiveness of OMB's process for waiving selected IoT cybersecurity requirements.³⁶ This is the third in a series of three reports. Previously, in December 2024, we reported on guidance for securely procuring IoT and agencies' progress in addressing IoT cybersecurity and waiver requirements.³⁷ We found that, out of the 23 CFO Act agencies in our review,³⁸ three had established inventories of their covered IoT assets, an OMB definition of IoT that includes some technologies that are traditionally called OT.³⁹ We

³³Title II of Pub. L. 115-390.

³⁴The council is chaired by a senior-level official from OMB. It includes representatives from GSA, DHS, the Office of the Director of National Intelligence, and the Departments of Justice, Defense, and Commerce.

³⁵As of July 2026, one such order has been issued and applies to the intelligence community.

³⁶Internet of Things Cybersecurity Improvement Act of 2020, Public Law No: 116-207 § 8(a)-(b), 134 Stat. 1006 (Dec. 4, 2020), 15 U.S.C. § 278g-3e(c).

³⁷[GAO-25-107179](#).

³⁸Our previous report covered the 23 civilian CFO Act agencies as covered by the act. As previously noted, USAID was excluded from our review for this report due to its recent significant workforce and operational reductions.

³⁹In January 2025, OMB dropped the use of the phrase "covered IoT" and directed agencies to inventory both IoT and OT devices that interact with the physical world.

also found that ten agencies planned to complete their inventories by the end of September 2024, three planned to complete their inventories by the end of September 2025, six had no time frame for completion, and one agency stated that it did not plan to create an inventory because it did not use covered IoT within its environment. In addition, we noted that none of the six reported waivers were consistent with the IoT cybersecurity requirements. Further, we found that OMB did not verify any of the reported waiver data and reported erroneous information. Accordingly, we made a total of 11 recommendations, including one recommendation to OMB and 10 recommendations to nine civilian agencies, to address legislative requirements related to IoT. As of July 2026, eight recommendations have been implemented.

In December 2022, we reported on cybersecurity risks associated with IoT and OT, including in selected key critical infrastructure areas.⁴⁰ We found that while guidance and resources had been developed to help manage cybersecurity risks to IoT and OT devices, selected sector risk management agencies (SRMA) lacked IoT- and OT-specific metrics to measure the effectiveness of their efforts. We also found that none of the selected SRMAs had conducted sector-wide risk assessments specific to IoT and OT devices. In addition, we noted that OMB had not yet established a standardized IoT device cybersecurity waiver process for the CIOs of covered federal agencies, as required by law. Accordingly, we made four recommendations to the selected SRMAs regarding the establishment and use of metrics to assess cybersecurity efforts. We made four additional recommendations regarding evaluating sector IoT and OT efforts. As of July 2026, three of the eight recommendations have been implemented. We also made one recommendation to OMB regarding issuing an IoT cybersecurity waiver process, as required by the act. In December 2022, OMB implemented the recommendation with the issuance of guidance in the form of a memorandum.⁴¹ Appendix I provides further details of the status of recommendations from our previous IoT reports.⁴²

⁴⁰[GAO-23-105327](#).

⁴¹Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-23-03 (Washington, D.C.: Dec. 2, 2022).

⁴²[GAO-25-107179](#) and [GAO-23-105327](#).

Guidance and Best Practices Can Assist Agencies in Securely Procuring Networked Devices

Federal agencies, including OMB, DHS, and NIST, have issued guidance, directives, regulations, and published recommended best practices to help federal agencies securely procure networked devices, among other things. Our prior reports under the act provide a detailed overview of these practices.⁴³ Guidance and key best practices from these agencies, as well as more recent updates issued since September 2024, are noted below.

OMB. The agency has issued various memoranda that provide cybersecurity requirements, including requiring agencies to secure and manage networked devices. Specifically, in December 2022, in response to the act and our December 2022 recommendation, OMB issued a memorandum for agencies to follow in requesting waivers.⁴⁴ This memorandum was rescinded by a December 2023 memorandum,⁴⁵ which, among other things: (1) clarified the IoT cybersecurity waiver process; (2) introduced the concept of covered IoT, which included both IoT and connected OT; and (3) required agencies to develop inventories of the IoT covered by OMB's guidance by September 2024, including the identification of the critical functions of the technologies.

OMB's most recent memorandum on networked device cybersecurity was issued in January 2025.⁴⁶ It provides additional guidance on identifying and securing networked IoT and OT devices. Among other things, the memorandum (1) clarified the scoping and definitions of networked devices; (2) directed agencies to maintain an updated enterprise-wide inventory of their networked IoT and OT assets that includes eight key categories of information (such as an asset description, manufacturer information, and software version) for each device; and (3) provided a standardized process for agencies to follow in determining whether to grant a waiver under the act. OMB has not issued an updated memorandum on networked device cybersecurity for fiscal year 2026.⁴⁷

⁴³[GAO-25-107179](#) and [GAO-23-105327](#).

⁴⁴Office of Management and Budget, Memorandum M-23-03.

⁴⁵Office of Management and Budget, Memorandum M-24-04.

⁴⁶Office of Management and Budget, Memorandum M-25-04, which also rescinded Memorandum M-24-04.

⁴⁷OMB did not respond to our February and June 2026 requests for updated information on the status of its guidance.

DHS and CISA. As discussed earlier, FISMA authorized DHS, in consultation with OMB, to develop and oversee the implementation of compulsory directives.⁴⁸ These are referred to as binding operational directives and cover non-national-security executive branch civilian agencies.⁴⁹ These directives require agencies to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.

In February 2020, DHS, in cooperation with the IT Government Coordinating Council (an interagency coordinating group) and the IT Sector Coordinating Council (an industry-led council), published a guide to help organizations involved in the acquisition lifecycle make risk-based acquisition decisions regarding secure IoT.⁵⁰ This voluntary guide is intended to highlight areas of elevated risk resulting from the software-enabled and connected aspects of IoT technologies and their role in the physical world and designed to be applicable to any critical infrastructure sector. It was designed to improve the effectiveness of supply chain, vendor, and technology evaluations prior to the purchase of IoT devices, systems, and services.

In January 2022, DHS's CISA issued a binding operational directive requiring agencies to address known exploited vulnerabilities in federal systems.⁵¹ In implementing this effort, CISA is responsible for the federal Coordinated Vulnerability Disclosure Process and Program and regularly issues notices that identify vulnerabilities in devices. In addition, it coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with affected vendor(s). This includes new vulnerabilities in industrial control systems (a type of OT), IoT, and medical devices, as well as traditional IT vulnerabilities.⁵² In June 2026, CISA issued a new binding operational

⁴⁸Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3076 (Dec. 18, 2014), codified at 44 U.S.C. § 3553(b)(2).

⁴⁹This responsibility is carried out by DHS's CISA.

⁵⁰Cybersecurity and Infrastructure Security Agency, *Internet of Things Security Acquisition Guidance: IT Sector*, (February 2020).

⁵¹Cybersecurity and Infrastructure Security Agency, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, BOD-22-01 (Washington, D.C.: Nov. 03, 2021).

⁵²For example, on May 28, 2026, CISA released advisories on 11 different control systems, ranging from data recorders used in the transportation sector; video recorders used in the commercial facilities, critical manufacturing, and emergency services sectors; to electric factory automation tools used in the critical manufacturing sector.

directive requiring agencies to prioritize addressing the highest risk vulnerabilities.⁵³ This clarifies the vulnerability remediation requirements introduced in January 2022 and creates a priority approach for agencies to use in making security updates based on various risk factors.

Additionally, in February 2026, CISA issued a binding operational directive requiring agencies to, among other things, inventory and subsequently decommission unsupported devices that are accessible from the public internet — referred to as “end of support”—or those devices that are no longer maintained by their vendors.⁵⁴ Devices covered by the directive include IoT devices.

Federal Acquisition Regulatory Council. The FAR Council has worked to strengthen the procurement rules around IoT devices. Specifically, in October 2023, the FAR Council published a proposed rule in the Federal Register that would require contracts for the management of a federal information system to specify any cybersecurity requirements necessary for IoT devices in accordance with NIST SP 800-213. The proposed rule would also implement the IoT Cybersecurity Improvement Act of 2020’s prohibition on agencies’ acquisition of an IoT device determined to be non-compliant with NIST standards and guidelines, absent a waiver by the agency head. Public responses to the initial rule were submitted to the FAR Council in December 2024. However, as of July 2026, acquisition program staff members continue to address comments on the proposed rule. We highlighted other proposed rules in our most recent report.⁵⁵

NIST. The agency’s Risk Management Framework is a risk-based approach that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle for federal

⁵³Cybersecurity and Infrastructure Security Agency, *Prioritizing Security Updates Based on Risk*, BOD-26-04 (Washington, D.C.: June 10, 2026) which revoked Cybersecurity and Infrastructure Security Agency, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, BOD-22-01 (Washington, D.C.: Nov. 3, 2021).

⁵⁴Cybersecurity and Infrastructure Security Agency, *Mitigating Risk From End-of-Support Edge Devices*, BOD-26-02 (Washington, D.C.: Feb. 5, 2026).

⁵⁵[GAO-25-107179](#).

agencies.⁵⁶ The framework also has many supporting documents, as well as detailed vulnerability disclosure guidance on specific IoT devices.

NIST has also issued a variety of documents providing recommended best practices for federal agencies to use in mitigating risk with the acquisition, procurement, and use of IoT and OT at all stages of a system's life cycle, some of which is in the process of being updated.⁵⁷ These documents include publications on the risk management of security, supply chain guidance, and consumer IoT, such as smart lightbulbs.

Further, NIST's guidelines in the special publication *Establishing IoT Device Cybersecurity Requirements* highlight a variety of approaches to securing IoT devices.⁵⁸ For example, if an IoT device lacks certain capabilities to support the information system's security controls, the capabilities lacking in the IoT device might be provided by other systems or system elements such as an IoT hub, cloud service, or mobile application. Alternatively, the organization might choose to implement compensating controls such as creating a segmented network for IoT. It could also reimplement existing controls such as changing a policy or procedure for a control in response to IoT device limitation. The guidance further notes that if risks introduced by the IoT device cannot be mitigated within the organization's risk tolerance level, the organization could accept these new risks or decide to not incorporate the IoT device into the information system.

In addition, NIST has also published a number of other documents that address secure IoT and OT, which are listed in appendix II. According to NIST officials, NIST is also in the process of developing guidance to assist healthcare organizations in securely integrating medical devices, a specialized form of IoT, into clinical environments. NIST officials stated that they anticipate the guidance will be issued in initial public draft form in 2027.

⁵⁶National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication (SP) 800-37 rev 2 (Gaithersburg, MD: Dec. 2018).

⁵⁷A prior GAO report under this mandate discussed a wide variety of NIST publications on the cybersecurity of IoT and OT. See [GAO-23-105327](#).

⁵⁸National Institute of Standards and Technology, Special Publication (SP) 800-213.

Most Agencies Have Not Fully Addressed OMB's Networked Device Cybersecurity Requirements

More than half of the 22 CFO Act agencies in our review have taken steps to address cybersecurity requirements for their networked devices, including establishing inventories, maintaining inventories, and including all required information in their inventories. However, only seven agencies had fully addressed all the requirements and about half of the inventories did not include all the information required by OMB.⁵⁹ Agencies cited various factors that contributed to the incomplete inventories, including competing priorities. As of August 2026, OMB had yet to issue updated guidance to agencies for implementing networked device requirements. Additionally, none of the 22 CFO Act agencies reported issuing IoT device waivers, as the act allows for under certain conditions.

Agencies Made Progress on Networked Device Inventories, but Most Did Not Fully Address OMB Requirements

As previously mentioned, OMB's December 2023 and January 2025 memoranda required the civilian CFO Act agencies to establish an enterprise-wide inventory of networked IoT and OT assets by the end of September 2024 and maintain it.⁶⁰ Further, agency networked device inventories were also to include, for each asset, eight categories of information: (1) asset identification, (2) asset description, (3) asset categorization, (4) the information system owner or information system security officer, (5) vendor or manufacturer information, (6) the software and firmware versions, (7) the network connectivity integrations and application programming interface, and (8) security controls. See figure 2 for a description of the eight required categories of information.

⁵⁹Office of Management and Budget, Memorandum M-24-04 and Office of Management and Budget, Memorandum M-25-04.

⁶⁰Office of Management and Budget, Memorandum M-24-04 and Office of Management and Budget, Memorandum M-25-04.

Figure 2: Office of Management and Budget's (OMB) Information Requirements for Agency Inventories of Networked Devices



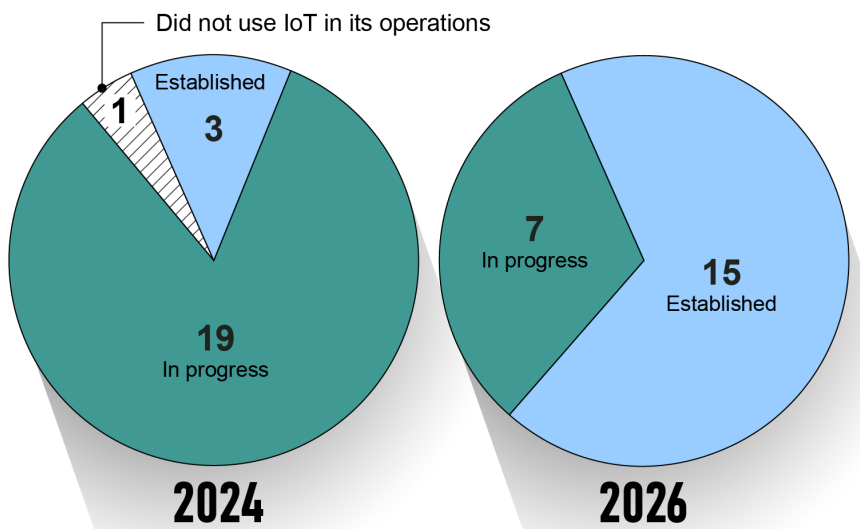
OMB's fiscal year 2025 Federal Information Security Modernization Act (FISMA) memorandum requires agencies to maintain an updated, enterprise-wide inventory inclusive of their agency's networked Internet of Things (IoT) and Operational Technology (OT) assets. Inventories must include:

-  **1) Asset identification:** All devices and systems that meet the provided definition of IoT or OT.
-  **2) Asset description:** Including make, model and any relevant specifications or configurations. Each asset should have a unique identifier, such as a serial or asset tag, to distinguish it from other assets.
-  **3) Asset categorization:** Factor in the device's function, location, and criticality. Include the following information:
 - a. Identification and/or description of specific agency FISMA and high value asset systems associated with the asset; and
 - b. The physical location of the asset (for example, a facility ID), if practicable, via the hardware asset management tool.
-  **4) Information system owner/information system security officer:** The individual or office responsible for the asset's management, administration, maintenance, and security.
-  **5) Vendor/manufacture information:** Include details about the vendor or manufacturer such as contact information and support channels.
-  **6) Software and firmware versions:** Record the installed software and firmware versions, including relevant patches or updates applied to the asset.
-  **7) Network connectivity, integrations and application programming interface information:** Specify network connection details, such as ports used by the asset or any software-based integrations.
-  **8) Security controls:** Describe physical and technological security controls, for example, user accounts and permissions, encryption of data at rest and in transit, physical controls, and authentication methods.

Sources: GAO analysis of OMB Memorandum M-25-04; GAO (shield check icon); ImageFlow/stock.adobe.com (header image). | GAO-26-108937

Agencies made progress in addressing OMB’s networked device inventory requirements. Specifically, from December 2024 to September 2026, the number of agencies that had established inventories increased from three to 15 (see figure 3).

Figure 3: Chief Financial Officer (CFO) Act Agency Progress in Establishing Initial Inventories of Networked Internet of Things (IoT) and Operational Technology Devices from December 2024 Through September 2026

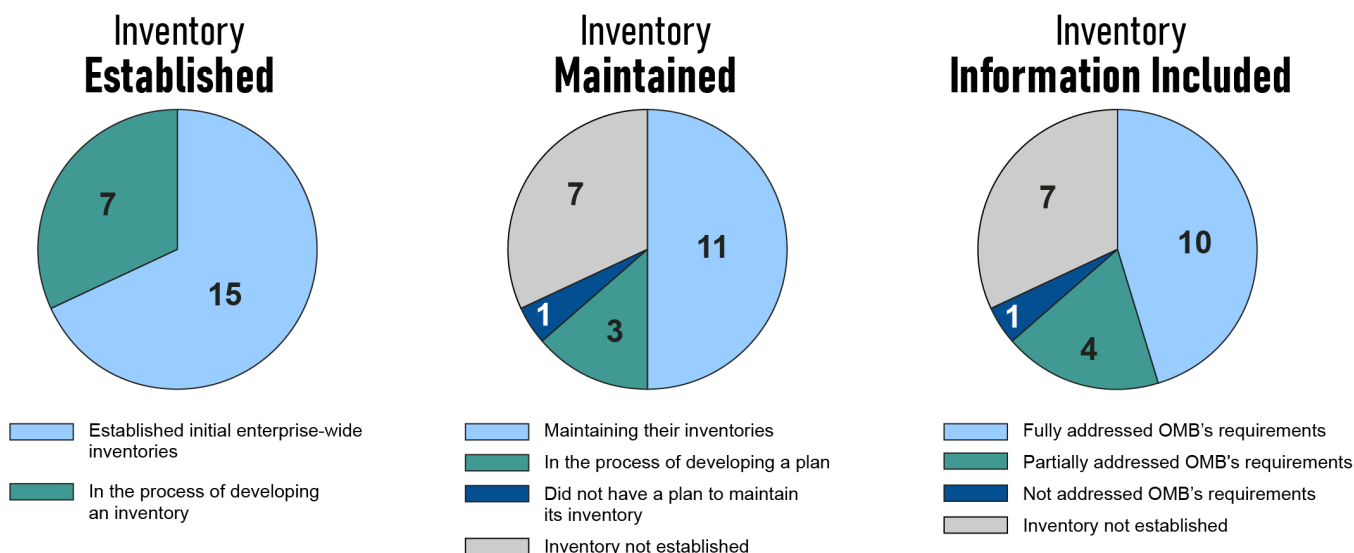


Source: GAO analysis of CFO Act agency documentation. | GAO-26-108937

Note: December 2024 inventory numbers included 23 CFO Act agencies’ data, while September 2026 inventory numbers included 22 CFO Act agencies’ data. Our 2026 analysis did not include the U.S. Agency for International Development, as the agency was not able to provide timely information due to a substantial reduction in personnel.

In addition, as of September 2026, 15 agencies had established an inventory; 11 agencies were maintaining the established inventories; and 10 agencies had included all eight required categories of information in their inventories (see figure 4).

Figure 4: Agency Efforts to Develop and Maintain Inventories of Networked Internet of Things (IoT) and Operational Technology (OT) Devices and Include All Required Information, as of September 2026



Source: GAO analysis of Chief Financial Officer (CFO) Act agency documentation. | GAO-26-108937

Establishing initial inventories. As of September 2026, of the 22 CFO Act agencies

- 15 agencies had established initial enterprise-wide inventories of their networked IoT and OT devices; and
- the remaining seven agencies were in the process of developing an inventory, three of which have open recommendations to develop inventories from our December 2024 report.⁶¹

Maintaining IoT inventories. As of September 2026, of the 15 CFO Act agencies that had established initial inventories

- 11 were maintaining their inventories,
- three agencies were in the process of developing a plan to maintain their inventories, and
- one did not have a plan to maintain its inventory.

⁶¹[GAO-25-107179](#).

Including required inventory information. As of September 2026, of the 15 CFO Act agencies that had established initial inventories

- 10 had included all the required information,
- four agencies had included some of the required information, and
- one agency had not included any of the required information.

As of September 2026, of the 22 CFO Act agencies, seven agencies had fully addressed all three of OMB's requirements—establishing inventories, maintaining inventories, and including all required information in their inventories. Table 1 provides a detailed overview of agencies' efforts to develop and maintain inventories of networked IoT and OT devices and include OMB's required categories of information. Further details on the extent to which agencies have addressed OMB's required inventory information is provided in appendix III.

Table 1: Status of Agencies' Efforts to Develop and Maintain Inventories of Networked Internet of Things (IoT) and Operational Technology (OT) Devices, as of September 2026

Agency ^a	Inventory established	Inventory maintained	Inventory information included	Description of agencies' inventory efforts
U.S. Department of Agriculture (USDA)	○	○	○	USDA officials stated that they conducted a pilot to inventory the agency's networked IoT and OT devices and have drafted plans to maintain it once established. They also stated that the agency has a system to scan its network for these devices; however, its implementation is on hold due to infrastructure changes and there is no timeline for establishing its inventory.
Department of Commerce	●	○	●	Commerce established its initial inventory in 2024, which included all OMB-required information. However, officials stated that individual components were responsible for maintaining their inventories. The department was also not maintaining its inventory across the entire enterprise on a recurring basis.
Department of Education	●	●	●	In March 2026, Education provided documentation demonstrating that it had established its initial inventory. The agency has also documented plans to maintain its inventory, which included all OMB-required information.
Department of Energy	●	●	◐	In March 2026, Energy provided documentation demonstrating that it had established its initial inventory. The agency has also documented plans to maintain its inventory. However, its inventory included only four of OMB's eight required categories of information, partially included one, and did not include the remaining three. According to officials, inventory information was removed in fiscal year 2025 due to the lack of meaningful data or sensitivity.
Department of Health and Human Services (HHS)	○	○	○	HHS officials stated that the agency was still evaluating potential solutions or alternatives to complete its initial inventory and is developing plans to maintain its inventory. However, officials stated there is no timeline for establishing its inventory. We previously made a recommendation for the department to complete its inventory effort. HHS has yet to address this recommendation.
Department of Homeland Security (DHS)	●	●	●	In May 2026, DHS provided documentation demonstrating that it had established its initial inventory. The agency has documented plans to maintain its inventory, which included all OMB-required information.
Department of Housing and Urban Development (HUD)	○	○	○	In June 2026, HUD officials stated that the agency was in the process of deploying new software for establishing and maintaining its inventory. However, officials stated that, while they plan to perform periodic validation of the data, they did not have a timeline for completing the software deployment.
Department of Justice	●	○	●	In March 2026, Justice provided documentation demonstrating that it had established its initial inventory. The inventory included all OMB-required information. However, the department was not maintaining its inventory on a recurring basis. Officials stated that this was due to significant staffing turnover and resource constraints over the last year.

Agency ^a	Inventory established	Inventory maintained	Inventory information included	Description of agencies' inventory efforts
Department of Labor	○	○	○	Labor officials stated that the inventory effort remains in progress because of resource constraints and competing mission-critical priorities. We previously made a recommendation for the department to complete its inventory effort. Labor has yet to address this recommendation.
Department of State	●	●	●	We reported in December 2024 that State had established its initial inventory. The agency has documented plans to maintain its inventory, which included all OMB-required information.
Department of the Interior	○	○	○	Interior officials stated the agency was in the process of establishing its inventory and plans to have its initial inventory completed by January 2027. Officials stated that the department is working on consolidating its inventory across the enterprise.
Department of Transportation	●	●	◐	In March 2026, Transportation provided documentation demonstrating that it had established its initial inventory. The agency had also documented plans to maintain its inventory. However, its inventory only included two of the eight required categories of information, partially included one, and did not include the remaining five. Officials stated that they are working on fully addressing OMB's requirements but did not have a timeline for doing so.
Department of the Treasury	●	◐	○	We reported in December 2024 that Treasury had established its initial inventory. Officials stated that they were in the process of documenting plans to maintain the department's inventory. However, they were not maintaining the inventory on a recurring basis and the established inventory did not include any of the OMB-required information.
Department of Veterans Affairs (VA)	○	○	○	VA officials stated that the agency was in the process of deploying a database to support its enterprise inventory. They added that full implementation for initial IoT inventory is planned for completion by the end of fiscal year 2026. We previously made a recommendation for the department to complete its inventory effort. VA has yet to address this recommendation.
Environmental Protection Agency (EPA)	●	●	●	EPA established its initial inventory in July 2025. The agency has documented plans to maintain its inventory, which included all OMB-required information.
General Services Administration (GSA)	●	●	●	In May 2025, GSA provided documentation demonstrating that it had established its initial inventory. The agency has documented plans to maintain its inventory, which included all OMB-required information.
National Aeronautics and Space Administration (NASA)	●	●	●	In May 2026, NASA provided documentation demonstrating that it had established its initial inventory. The agency has documented plans to maintain its inventory, which included all OMB-required information.
National Science Foundation (NSF)	○	○	○	As of March 2026, NSF officials stated that the agency had not yet established its initial inventory due to its building relocation and did not provide a timeline for establishing the inventory.

Agency ^a	Inventory established	Inventory maintained	Inventory information included	Description of agencies' inventory efforts
Nuclear Regulatory Commission (NRC)	●	●	◐	We reported in December 2024 that NRC had established its initial inventory. It has documented plans to maintain its inventory. However, its inventory only fully included two of the eight required categories of information, partially included three, and did not include the remaining three. Officials stated that they were in the process of implementing additional tools to capture the remaining categories but did not provide a timeline.
Office of Personnel Management (OPM)	●	●	●	In March 2026, OPM provided documentation demonstrating that it had established its initial inventory. The agency has documented plans to maintain its inventory, which included all OMB-required information.
Small Business Administration (SBA)	●	●	◐	In April 2026, SBA provided documentation demonstrating that it had established its initial inventory. The agency has documented plans to maintain its inventory. However, its inventory fully included two of the eight required pieces of information, partially included three, and did not include the remaining three. Officials did not provide a timeline for addressing all the requirements.
Social Security Administration (SSA)	●	◐	●	In March 2026, SSA provided documentation demonstrating that it had established its initial inventory. SSA officials stated that they are in the process of documenting plans to maintain the inventory. The initial inventory included all OMB-required information. However, SSA was not maintaining the inventory on a recurring basis. Officials stated that they were in the process of acquiring specific monitoring technologies to observe and report on the agency's inventories.

● = Fully addressed ◐ = Partially addressed ○ = Not addressed

Source: GAO analysis of Chief Financial Officer Act agency and Office of Management and Budget (OMB) documentation. | GAO-26-108937

^aAlthough we contacted the U.S. Agency for International Development, due to a substantial reduction in personnel, the agency was not able to provide timely information.

Various Factors Contributed to Agencies' Challenges in Addressing Inventory Requirements

Agencies cited several factors that continue to hinder their efforts to address OMB's and the act's networked device cybersecurity requirements, such as technical and resource constraints and competing priorities. For example, officials from the Department of Housing and Urban Development stated that the agency's new hardware asset management system identified over 160 IoT devices that were not reported by its legacy system. Moreover, some agency officials noted that it was not always clear to agencies how certain devices should be categorized. For example, while NASA had established an inventory, NASA officials noted that, in their experience, there are no asset discovery tools that have a reliable way of distinguishing between IT, IoT, and OT. They noted that this is due to the overlapping nature of technology and definitions. The officials also noted that there are

challenges with tools that use active queries against devices for asset discovery, which can disrupt or disable some sensitive systems.

As noted earlier, OMB is responsible for the oversight of the management of federal agencies' technologies, including enabling agencies to adopt IoT and OT, in a manner that enhances the agencies' missions.⁶² To this end, OMB is to oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including IoT devices).⁶³ Most agencies have not fully addressed OMB's networked device cybersecurity requirements, some of which were due in September 2024 after being established in December 2023 and updated in January 2025. However, OMB has yet to issue updated guidance to agencies that covers fiscal year 2026 and provide agencies with clear expectations on what is required to secure their networked IoT and OT devices. In the absence of such guidance, agencies are left without a clear imperative to prioritize implementation of the requirements or a timeline for doing so. Moreover, OMB did not oversee the implementation of its requirements regarding establishing and maintaining inventories of networked IoT and OT devices within an established time frame.⁶⁴

Updated inventories enable agencies to monitor and detect unauthorized, abnormal, or potentially malicious activities and ensure a more secure and resilient infrastructure. If agencies do not establish and maintain inventories of their networked IoT and OT technology assets that meet OMB's requirements, agency CIOs and Chief Information Security Officers may lack awareness of the number and type of connected devices in their systems and be unable to protect those systems from cyberattacks. Further, OMB's lack of guidance and oversight increases the risk that agencies will be challenged in applying appropriate security controls to vulnerable systems or make risk-based decisions about how to mitigate cybersecurity incidents—potentially compromising highly sensitive data and systems.

⁶²40 U.S.C. § 11302-03 (Clinger-Cohen Act); see also 44 U.S.C. § 3504 (Paperwork Reduction Act); 44 U.S.C. § 3602 (E-Government Act); 44 U.S.C. § 3553 (Federal Information Security Modernization Act of 2014, which largely superseded the Federal Information Security Management Act of 2002).

⁶³Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, §5(d), 134 Stat. 1004 (Dec. 4, 2020), 15 U.S.C. § 278g-3c.

⁶⁴OMB did not respond to our February and June 2026 requests for updated information on the status of its guidance and agencies' implementation of the requirements.

No Agencies Reported Waivers Under the IoT Cybersecurity Improvement Act of 2020

As previously discussed, OMB's January 2025 memorandum provides a standardized process for agencies to follow in determining whether to grant an IoT device waiver under the act.⁶⁵ Specifically, the memorandum defines when and how agencies could waive a prohibition against using IoT devices that do not comply with NIST's IoT standards and guidelines. The act requires that agency CIOs determine whether an IoT device that would otherwise be prohibited meets one of three waiver conditions.⁶⁶ OMB determined that the CIO can then justify such a determination in a signed memorandum to the head of the agency for their approval. OMB established the following waiver process:

- The agency head may issue a waiver of the prohibition on use or acquisition of the device in question.
- The waiver must include information about the solutions or platforms covered; a description of the purposes for which or the circumstances in which the device may be acquired or used; and the effective period of the waiver, which may not exceed 2 years.
- The CIOs must make these waivers available to OMB upon request and ensure that such waivers are documented in relevant system security plans and shared with acquisition officials for documentation in relevant contract files.⁶⁷

However, none of the 22 agencies in our review reported such a waiver. While one agency—HHS—reported a waiver in 2024, the agency subsequently removed those IoT devices from the system in question. As a result, that waiver is no longer relevant. In 2024, we recommended that OMB verify agency-reported IoT cybersecurity waivers.⁶⁸ Performing such verifications would ensure that any waivers issued in the future are appropriately documented and approved.

Conclusions

Cyber threats to networked IoT and OT devices represent a significant national security challenge. In response to these threats, the federal government has responded with legislation to ensure device security, as

⁶⁵Office of Management and Budget, Memorandum M-25-04.

⁶⁶The three waiver conditions are (1) the waiver is necessary in the interest of national security; (2) procuring, obtaining, or using the IoT device is necessary for research purposes; or (3) the device is secured using alternative and effective methods appropriate to its function.

⁶⁷Office of Management and Budget, Memorandum M-25-04.

⁶⁸[GAO-25-107179](#).

well as guidance and best practices to help agencies better secure their technology. Further, some agencies have made progress in their mandated efforts to develop and maintain complete inventories of networked devices since we last reported on this issue in December 2024. However, as of September 2026, seven of the 22 agencies had not yet established initial device inventories which were due almost 2 years ago (in September 2024), four agencies with complete inventories were not properly maintaining their repositories, and five agencies had not included all of the OMB-required information in their inventories.

Establishing inventories of networked devices will allow agencies to have a clear understanding of the number and type of devices connected to their information systems. Additionally, maintaining complete, up-to-date inventories of these networked IoT and OT technology assets can better position agency CIOs and Chief Information Security Officers to know which of their agency's devices are connected to their information systems—and have ready access to information on the attributes of each of those devices. OMB has not issued updated guidance to agencies that covers fiscal year 2026, leaving agencies without a clear imperative to prioritize implementation of the networked device cybersecurity requirements or a timeline for doing so. Moreover, OMB did not oversee the implementation of its cybersecurity priorities for networked IoT and OT devices. In the absence of current guidance and oversight, agencies that have not yet fully met the requirements may continue to struggle to apply appropriate security controls to their devices, make informed risk-based decisions about mitigating security threats, and respond appropriately in the event of a cybersecurity incident.

Recommendation for Executive Action

The Director of OMB should issue updated cybersecurity guidance, to include requirements for networked IoT and OT devices, and oversee agencies' implementation of the requirements. The guidance should include a clear imperative to prioritize implementation of the networked device requirements and a timeline for doing so. (Recommendation 1)

Agency Comments

We provided a draft of this report to OMB, to which we made a recommendation, and the 22 civilian CFO Act agencies for their review and comment. OMB did not provide comments on the draft report. We received responses from all 22 agencies, as summarized below.

Four agencies—Commerce (NIST), DHS (CISA), NASA, and OPM — provided technical comments, which we incorporated as appropriate. The other 18 agencies—the Departments of Agriculture, Education, Energy, Health and Human Services, Housing and Urban Development, the

Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Science Foundation; Nuclear Regulatory Commission; Small Business Administration; and the Social Security Administration—stated that they had no comments.

We are sending copies of this report to the appropriate congressional committees, the Director of OMB, the heads of the 22 civilian CFO Act agencies, and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Andrew R. Garbarino
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable James Comer
Chairman
The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Appendix I: Prior GAO Recommendations Related to the Internet of Things Cybersecurity Improvement Act of 2020

Our prior reports under the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 contain recommendations addressing legislative requirements related to IoT.¹ As of August 2026, three recommendations from our December 2024 report had not been implemented, and five recommendations from our December 2022 report had not been implemented.²

In December 2024, we reported on guidance for securely procuring IoT and on agencies' progress in addressing IoT cybersecurity and waiver requirements.³ We made a total of 11 recommendations, including one recommendation to the Office of Management and Budget (OMB) and 10 recommendations to nine civilian Chief Financial Officer Act (CFO Act) agencies. As of August 2026, eight of the 11 recommendations had been implemented by the agencies. Table 2 shows the implementation status for the open recommendations under our December 2024 report.

¹GAO, *Internet of Things: Federal Actions Needed to Address Legislative Requirements*, [GAO-25-107179](#) (Washington, D.C.: Dec. 4, 2024) and *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, [GAO-23-105327](#) (Washington, D.C.: Dec. 1, 2022).

²[GAO-25-107179](#) and [GAO-23-105327](#).

³[GAO-25-107179](#).

**Appendix I: Prior GAO Recommendations
Related to the Internet of Things Cybersecurity
Improvement Act of 2020**

Table 2: Open Recommendations on Addressing Internet of Things (IoT) Legislative Requirements from [GAO-25-107179](#), as of August 2026

Agency	Open recommendation	Status
Department of Health and Human Services (HHS)	The Secretary of HHS should direct the Chief Information Officer (CIO) to complete the covered IoT inventory within the revised time frame it has proposed. ^a (Recommendation 3)	In June 2025, agency officials stated that HHS was reevaluating potential solutions and alternatives for completing its IoT inventory and that the completion date for the effort was yet to be determined. In April 2026, HHS officials stated that HHS was still evaluating these potential solutions and is developing plans to maintain its inventory.
Department of Labor (Labor)	The Secretary of Labor should direct the CIO to establish a plan and time frame for completing the covered IoT inventory, as directed by the Office of Management and Budget (OMB). (Recommendation 4)	In April 2025, agency officials noted that, due to limited resources and competing priorities (such as zero trust initiatives and implementing OMB's Memorandum M-24-15: <i>Modernizing the Federal Risk and Authorization Management Program</i>), progress on establishing a plan and time frame for completing the covered IoT inventory was delayed. In May 2026, Labor officials stated that its inventory effort remains in progress because of resource constraints and competing mission-critical priorities.
Department of Veterans Affairs (VA)	The Secretary of Veterans Affairs should direct the CIO to establish a plan and time frame for completing the covered IoT inventory, as directed by OMB. (Recommendation 5)	In May 2025, agency officials stated that VA was in the process of updating the policies and contract security processes that support the procurement of IoT and medical devices. They also described activities to address OMB's covered IoT inventory requirements, including verifying IoT asset data. The planned efforts were scheduled to be completed by September 30, 2025. In March 2026, VA officials stated that the agency planned to have its initial inventory established by the end of 2026.

Source: GAO-25-107179 and GAO analysis of agency-reported data. | GAO-26-108937

^aCovered IoT was an administrative definition of IoT used by OMB that included some technologies that are traditionally called operational technology (OT). In January 2025, OMB dropped the use of the phrase "covered IoT" and directed agencies to inventory both networked IoT and OT devices that interact with the physical world.

In December 2022, we reported⁴ on cybersecurity risks associated with IoT and operational technology (OT),⁵ including in selected key critical infrastructure areas.⁶ We made a total of nine recommendations, one recommendation to OMB and eight recommendations to four civilian CFO

⁴[GAO-23-105327](#).

⁵OT are programmable systems or devices that interact with the physical environment (or manage such devices). These could include control systems in factories or building automation.

⁶The term "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

**Appendix I: Prior GAO Recommendations
Related to the Internet of Things Cybersecurity
Improvement Act of 2020**

Act agencies. As of July 2026, four of the nine recommendations had been implemented by the agencies. Table 3 shows the implementation status for the five open recommendations under our December 2022 report, [GAO-23-105327](#).

Table 3: Open Recommendations on Addressing Internet of Things (IoT) Legislative Requirements from [GAO-23-105327](#), as of August 2026

Agency	Open recommendation	Status
Department of Energy	The Secretary of Energy, as sector risk management agency (SRMA) for the energy sector, should direct the Director of the Office of Cybersecurity, Energy Security, and Emergency Response to use the National Infrastructure Protection Plan (National Plan) to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and operational technology (OT) environments. (Recommendation 1)	In April 2023, Energy officials noted that the agency was working with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) on updating the National Plan. They added that once the National Plan was updated, the agency would work toward updating its sector-specific plan. Officials stated that the sector-specific plan is estimated to be completed one year after the updated National Plan is published. According to the President's <i>National Security Memorandum on Critical Infrastructure Security and Resilience</i> in April 2024, the updated National Plan was due by April 2025. However, as of July 2026, activity on the National Plan is on hold pending the completion of a review of critical infrastructure policy and it is unclear when work on the National Plan will resume.
Department of Energy	The Secretary of Energy, as SRMA for the energy sector, should direct the Director of the Office of Cybersecurity, Energy Security, and Emergency Response to include IoT and OT devices as part of the risk assessments of their sector's cyber environment. (Recommendation 2)	In July 2024, Energy officials stated that it considered IoT and OT devices as part of a sector risk analysis completed in collaboration with industry through the utilization of Lawrence Livermore National Laboratory. Officials noted that the work is to be incorporated into a sector risk assessment that has been delayed due to delays with CISA's update to the national critical infrastructure plan. As of July 2026, activity on the National Plan is on hold pending the completion of a review of critical infrastructure policy and it is unclear when work on the National Plan will resume.
Department of Health and Human Services (HHS)	The Secretary of Health and Human Services, as SRMA for the healthcare and public health sector, should direct the Assistant Secretary for Preparedness and Response to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 3)	In May 2023, HHS officials stated that the Assistant Secretary for Preparedness and Response (ASPR) was awaiting the release of the National Plan to update the sector-specific plan for the Healthcare and Public Health Sector. HHS also stated that while ASPR does not have the authority to mandate reporting or the resources to support a comprehensive effort to track the implementation or success of any activities related to IoT and OT, it will include considerations about IoT and OT as part of its all-hazards approach when it updates the sector-specific plan. In addition, the agency stated that it will continue to consult and coordinate with ASPR, other relevant HHS offices, and other federal agencies such as DHS/CISA and the Department of Commerce/National Institute of Standards and Technology (NIST) to promote a collaborative approach to the larger cross-sector landscape. While the updated National Plan was due by April 2025, as of July 2026, HHS continues to work on the sector-specific plan and does not have a timeline associated with the release of the plan.

**Appendix I: Prior GAO Recommendations
Related to the Internet of Things Cybersecurity
Improvement Act of 2020**

Agency	Open recommendation	Status
Department of Homeland Security (DHS)	The Secretary of Homeland Security should direct the Administrator of the Transportation Security Administration and the Commandant of the U.S. Coast Guard to jointly work with the Department of Transportation's Office of Intelligence, Security and Emergency Response, as co-SRMAs for the transportation systems sector, to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 5)	In May 2023, DHS stated that the Transportation Security Administration, in coordination with the Coast Guard and other DHS offices and divisions and the Department of Transportation, were in the process of updating the 2015 transportation systems sector-specific plan. DHS stated that the publication of the revised plan is contingent on the release of the revised Presidential Policy Directive 21 (PPD-21) and the National Plan. The President's National Security Memorandum on Critical Infrastructure Security and Resilience (the update to PPD-21) was released in April 2024 and the updated National Plan was due by April 2025. As of July 2026, the plan has not been released. DHS officials originally stated that the co-SRMAs anticipate releasing the final updated sector-specific plan within six to eight months of the completion of the National Plan. However, as of July 2026, activity on the National Plan is on hold pending the completion of a review of critical infrastructure policy and it is unclear when work on the National Plan will resume. Given this, DHS officials reported in July 2026 that the co-SRMAs intend to review their draft Sector Risk Management Plan and identify a path forward to revise, re-write, or identify similar efforts to leverage previous work.
Department of Transportation	The Secretary of Transportation should direct the Director, Office of Intelligence, Security and Emergency Response to jointly work with the Administrator of DHS's Transportation Security Administration and the Commandant of the U.S. Coast Guard, as co-SRMAs for the transportation systems sector, to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 7)	In April 2023, Transportation officials reported that, in coordination with co-SRMA partners at DHS, the agency is developing an update to the 2015 sector-specific plan. Officials noted that the department plans to include metrics for measuring the effectiveness of efforts to enhance the cybersecurity of the sector's IoT and OT environments. In addition, the department stated that the update is dependent on DHS finalizing the National Plan to ensure that the sector-specific plan aligns with any substantive changes in the new National Plan. According to the President's National Security Memorandum on Critical Infrastructure Security and Resilience in April 2024, the updated National Plan was due by April 2025. However, as of July 2026, the plan still has not been released. In April 2026, Transportation officials reported that they expected to have a plan in place by the end of 2026. However, as of July 2026, activity on the National Plan is on hold pending the completion of a review of critical infrastructure policy and it is unclear when work on the National Plan will resume. Given this, DHS officials reported in July 2026 that the Transportation Security Administration, the Department of Transportation, and the U.S. Coast Guard intend to review the draft Sector Risk Management Plan and identify a path forward to revise, re-write, or identify similar efforts to leverage previous work.

Source: GAO-23-105327 and GAO analysis of agency-reported data. | GAO-26-108937

Appendix II: Key National Institute of Standards and Technology Publications

The National Institute of Standards and Technology (NIST) publishes a wide variety of recommended best practices in the form of guidance that are relevant to Internet of Things (IoT) and operational technology (OT) devices (see table 4). Our prior reports under the Internet of Things Cybersecurity Improvement Act of 2020 provide a more detailed overview of these practices.¹

Table 4: Key National Institute of Standards and Technology (NIST) Publications Providing Guidelines for the Secure Procurement of Internet of Things (IoT) and Related Devices, as of July 2026

Publication (release date)	Description and status
Special Publication (SP) 800-82 Revision 3, <i>Guide to Operational Technology (OT) Security</i> (September 2023)	Intended to describe how to apply the NIST Risk Management Framework (SP 800-37 Revision 2) to OT and provide an overlay of the NIST SP 800-53 Revision 5 control catalog to further help organizations apply the NIST controls to OT. According to NIST officials, the institute plans to update the guidance to version 4 with an initial public draft in late 2026, barring any significant technical issues.
SP 800-161r1, <i>Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations</i> (May 2022)	Intended to provide organizations with a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures for supply chain risk management. ^a
SP 800-213, <i>IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements</i> (November 2021)	Intended to provide organizations with a process to consider cybersecurity for IoT devices and products in their systems. The document helps organizations identify and select appropriate cybersecurity requirements for IoT devices and products based on the functionality of the product and cybersecurity context of the system. NIST issued an initial public draft of SP 800-213 revision 1 in June 2026; barring any significant technical issues, NIST officials stated that they plan to issue revision 1 in final form in late 2026.
SP 800-213A, <i>IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog</i> (November 2021)	Intended to provide agencies with a catalog of IoT device cybersecurity capabilities and non-technical supporting capabilities that can help organizations as they use SP 800-213 to determine and establish device cybersecurity requirements. NIST officials stated they plan to update the guidance with an initial public draft in the winter of 2026-27, barring any significant technical issues.
SP 800-53, Revision 5, <i>Security and Privacy Controls for Information Systems and Organizations</i> (September 2020)	Intended to help federal agencies protect organizational operations and assets, individuals, other organizations, and the nation from a diverse set of threats and risks. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. It provides a catalog of security and privacy controls for federal information systems and a process for selecting controls to protect organizational operations and assets, which includes IoT and OT.

¹GAO, *Internet of Things: Federal Actions Needed to Address Legislative Requirements*, [GAO-25-107179](#) (Washington, D.C.: Dec. 4, 2024) and *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, [GAO-23-105327](#) (Washington, D.C.: Dec. 1, 2022).

**Appendix II: Key National Institute of
Standards and Technology Publications**

Publication (release date)	Description and status
NIST Interagency Report 8228, <i>Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks</i> (June 2019)	Intended to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' life cycles. It identifies considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT devices and describes ways that organizations can mitigate IoT cybersecurity and privacy risks.
SP 800-37, Revision 2, <i>Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy</i> (September 2018)	Intended to help organizations understand NIST's Risk Management Framework and provide guidelines for applying the framework to information systems and organizations. It provides a disciplined, structured, and flexible process for managing security and privacy risks that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

Source: GAO analysis of NIST publications. | GAO-26-108937

^aNIST defines the supply chain as a linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.

Appendix III: Extent to Which Agencies Have Implemented Networked Device Inventory Information Requirements

The Office of Management and Budget requires Chief Financial Officer Act agencies to include eight categories of information in the agencies' inventories of networked Internet of Things (IoT) and operational technology (OT) devices. Table 5 provides information on the status of each agency's efforts as of September 2026.

Table 5: Extent to Which Chief Financial Officers (CFO) Act Agencies Included Eight Categories of Information Required by OMB in Their Networked Device Inventories, as of September 2026

Agency	Overall rating	1	2	3	4	5	6	7	8
U.S. Department of Agriculture ^a	○	○	○	○	○	○	○	○	○
Department of Commerce	●	●	●	●	●	●	●	●	●
Department of Education	●	●	●	●	●	●	●	●	●
Department of Energy	◐	●	●	◐	●	●	○	○	○
Department of Health and Human Services ^a	○	○	○	○	○	○	○	○	○
Department of Homeland Security	●	●	●	●	●	●	●	●	●
Department of Housing and Urban Development ^a	○	○	○	○	○	○	○	○	○
Department of Justice	●	●	●	●	●	●	●	●	●
Department of Labor ^a	○	○	○	○	○	○	○	○	○
Department of State	●	●	●	●	●	●	●	●	●
Department of the Interior ^a	○	○	○	○	○	○	○	○	○
Department of Transportation	◐	●	◐	○	○	●	○	○	○
Department of the Treasury	○	○	○	○	○	○	○	○	○
Department of Veterans Affairs ^a	○	○	○	○	○	○	○	○	○

**Appendix III: Extent to Which Agencies Have
Implemented Networked Device Inventory
Information Requirements**

Environmental Protection Agency	●	●	●	●	●	●	●	●	●
General Services Administration	●	●	●	●	●	●	●	●	●
National Aeronautics and Space Administration	●	●	●	●	●	●	●	●	●
National Science Foundation ^a	○	○	○	○	○	○	○	○	○
Nuclear Regulatory Commission	◐	●	◐	◐	●	◐	○	○	○
Office of Personnel Management	●	●	●	●	●	●	●	●	●
Small Business Administration	◐	●	○	◐	○	◐	●	◐	○
Social Security Administration	●	●	●	●	●	●	●	●	●

● = Fully addressed ◐ = Partially addressed ○ = Not addressed

Source: GAO analysis of CFO Act agency and Office of Management and Budget (OMB) documentation. | GAO-26-108937

Notes: While we contacted the U.S. Agency for International Development, due to a substantial reduction in personnel, the agency was not able to provide timely information.

OMB-required inventory categories: (1) Asset Identification; (2) Asset Description; (3) Asset Categorization; (4) Information System Owner; (5) Vendor/ Manufacturer Information; (6) Software and Firmware Versions; (7) Network Connectivity, Integrations and Application Programming Interface Information; and (8) Security Controls

^aAgency has not yet established an initial inventory.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Neela Lakhmani (Assistant Director), Kara Lovett Epperson (Analyst-in-Charge), Olivia Adams, Alina Budhathoki, Christopher Businsky, and Jess Lionne made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.